Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of Emergency Broadband Benefit Program	WC Docket No. 20-445

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Elizabeth Laird
Cody Venzke

Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, D.C. 20005
202.637.9800

January 25, 2021

Executive Summary

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Public Notice issued by the Wireline Competition Bureau, seeking public comment on a new Emergency Broadband Benefit Program, as established by the Consolidated Appropriations Act, 2021.

CDT applauds the efforts of Congress and the Commission to close the homework gap and bridge the digital divide and offers these comments on how to connect students and families while protecting their privacy. The Program provides critical resources to connect students learning from home to their lessons and to help make broadband affordable for low-income families. However, a failure to garner students' and families' trust can chill participation and hamper the Program's effectiveness. To help earn that trust, the Commission should protect students' and families' privacy by:

- Using school enrollment data—rather than sensitive individual eligibility data—when possible to verify students' participation in the National School Lunch Program or the School Breakfast Program, especially when the school has adopted the Community Eligibility Provision.
- Fully enabling students' participation in the Program by providing cybersecurity and digital literacy training and clarifying disparate applications of the monitoring requirement of the Children's Internet Protection Act.

In addition to these education-specific recommendations, CDT also suggests that the Commission adopt privacy-forward and equitable data practices to ensure the Program achieves its goal of closing the digital divide while protecting individual rights by:

- Limiting broadband providers' data collection and use under the Program.
- Avoiding inadvertent disclosures of personal information while meeting data reporting and accountability requirements.
- Prioritizing marginalized communities and students under the Program through the review of applications, outreach, and technical support.

Table of Contents

Introduction

On December 27, 2020, the President signed the Consolidated Appropriations Act, 2021,[1] which among many other provisions, provided $3.2 billion in funds for an Emergency Broadband Benefit Program[2] to reimburse broadband providers for discounts provided to certain low-income households.[3]

The Act's eligibility requirements for the Program depend to a large extent on education data.[4] For example, under the Act, a low-income household is eligible to participate in the Program if at least one member has been approved to participate in the National School Lunch Program (NSLP) under the Richard B. Russell National School Lunch Act[5] or the School Breakfast Program (SBP) under the Child Nutrition Act of 1966.[6] A household may also be eligible for the Program if it qualifies for the Commission's existing Lifeline program.

The Act's verification procedures also incorporate education data.[7] For example, under the Act, broadband providers may verify a household's eligibility by "rely[ing] on" schools to "verify the eligibility of a household based on the participation of the household in the free and reduced price lunch program or the school breakfast program."[8] Among other things, broadband providers may also verify household eligibility by using the Lifeline National Eligibility Verifier (National Verifier) and National Lifeline Accountability Database (NLAD), operated by the Universal Service Administrative Company (USAC).[9]

As directed by the Act, on January 4, 2021, the Wireline Competition Bureau issued a Public Notice[10] asking for public comment on how to establish the Program to distribute the

[1] Consolidated Appropriations Act, 2021, Pub. L. 116-260 (2020) [hereinafter Consolidated Appropriations Act], *available at* https://www.congress.gov/bill/116th-congress/house-bill/133/text.
[2] Consolidated Appropriations Act, sec. 904(i).
[3] *Id.*, sec. 904(b)(1).
[4] *Id.*, sec. 904(a)(6).
[5] 42 U.S.C. § 1751 *et seq.*
[6] 42 U.S.C. § 1773.
[7] Consolidated Appropriations Act, sec. 904(b)(2).
[8] *Id.*, sec. 904(b)(2)(C).
[9] *Id.*, sec. 904(b)(2)(A).
[10] *Wireline Competition Bureau Seeks Comment on Emergency Broadband Connectivity Fund Assistance*, Public Notice, DA 21-6 (WCB Jan. 4, 2021) [hereinafter Public Notice], *available at* https://www.fcc.gov/document/fcc-seeks-comment-new-emergency-broadband-benefit-program.

emergency funds. In establishing the Program, the Commission should take the following steps to protect privacy and equity in order to earn users' trust and ensure the Program's success.[11]

I. Use School Enrollment Data—Rather than Sensitive Individual Eligibility Data—When Possible to Verify Students' Participation in the National School Lunch Program or the School Breakfast Program, Especially When the School Has Adopted the Community Eligibility Provision

The Act permits broadband providers to rely on schools to verify participation in the National School Lunch Program or the School Breakfast Program. The Bureau seeks comment on what information a broadband provider should collect from schools and submit to meet this verification requirement.[12]

Data on individual students' eligibility for the NSLP or SBP will often not be available; even if it is, it may be incomplete and will include sensitive information such as families' socioeconomic status and participation in government programs. Consequently, the Commission should discourage broadband providers from seeking those data on an individual level. Instead, broadband providers should verify eligibility for the Program by relying on school enrollment data when possible. When collecting individual data is the only option, such data collection should be accompanied by communication with families, parental consent, and additional safeguards such as data-sharing agreements, data minimization, and best security practices.

A. Individual NSLP or SBP Eligibility Data Are Often Unavailable or Incomplete and Pose Challenges to Student Privacy

Individual-level data on students' eligibility for the NSLP or SBP may not be available and, even if it is, it may pose challenges to student privacy. First, many schools will not be able

[11] *Cf.* Sarah Holder, *Contact Tracing Is Having a Trust Crisis*, CityLab (Aug. 12, 2020), https://www.bloomberg.com/news/articles/2020-08-12/why-are-americans-so-uneasy-about-contact-tracing; Craig Timberg, *Most Americans Are Not Willing or Able to Use an App Tacking Coronavirus Infections*, Wash. Post (Apr. 29, 2020), https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/ ("A major source of skepticism about the infection-tracing apps is distrust of Google, Apple and tech companies generally, with a majority expressing doubts about whether they would protect the privacy of health data.").

[12] Public Notice at 7.

to provide individual-level data. As the Public Notice observes,[13] many schools do not collect individual eligibility applications, but instead provide free lunches to all students through the Community Eligibility Provision (CEP). In fact, as of 2019, 64.6% of all eligible schools had adopted community eligibility.[14] That means that a large portion of schools no longer collect student-level data on who is eligible for free or reduced-price meals.

For the remaining portion of schools that do not participate in CEP, individual-level data may be incomplete or inaccurate. For example, due to being physically closed, "[m]any school districts are providing school meals through the Summer Food Service Program . . . rather than through the National School Lunch Program," and consequently, "may not have collected school applications at the start of the school year."[15] Those schools that have collected applications have also experienced marked drops in NSLP participation due to the pandemic.[16] Consequently, relying on individual applications for eligibility in the NSLP or SBP may severely underestimate the number of households that are eligible for participation in the Emergency Broadband Benefit Program.

Moreover, collecting personally identifiable information threatens student privacy and may implicate student privacy laws. Students' participation in the NSLP or SBP carries implied information about families' socioeconomic status and participation in federal and state benefit programs[17] and is consequently particularly sensitive. Because of its sensitivity, that information is protected not only by the Family Educational Rights and Privacy Act (FERPA),[18] but also the

---

[13] Public Notice at 7 ("We seek comment on how households with students in these Community Eligibility Provision schools should be considered eligible households for the Emergency Broadband Benefit Program.").
[14] Food Research & Action Center, Community Eligibility: The Key to Hunger-Free Schools (2019), *available at* https://frac.org/wp-content/uploads/community-eligibility-key-to-hunger-free-schools-sy-2018-2019.pdf.
[15] USDA, School Year 2020-2021 P-EBT Questions & Answers at 3 (Nov. 16, 2020), *available at* https://www.fns.usda.gov/snap/state-guidance-coronavirus-pandemic-ebt-pebt; *FNS Frequently Asked Questions*, USDA (Apr. 15, 2020), https://www.fns.usda.gov/disaster/pandemic/covid-19/fns-frequently-asked-questions ("All states currently have a waiver in place that allows schools to serve meals through the Summer Food Service Program (SFSP) or Seamless Summer Option (SSO) during unexpected school closures, such as the current national emergency.").
[16] Cory Turner, *'Children Are Going Hungry': Why Schools Are Struggling to Feed Students*, NPR (Sept. 8, 2020), https://www.npr.org/2020/09/08/908442609/children-are-going-hungry-why-schools-are-struggling-to-feed-students.
[17] USDA, Eligibility Manual for School Meals at 22 (July 18, 2017), *available at* https://www.fns.usda.gov/cn/eligibility-manual-school-meals (describing eligibility based on income and household size or participation in government programs).
[18] 20 U.S.C. § 1232g; 34 C.F.R. § 99.30.

Richard B. Russell National School Lunch Act, which limits disclosure without parental consent to a few enumerated recipients responsible for implementing federal and state education and nutritional programs.[19] Disclosure of a student's participation in the NSLP or SBP may run afoul of those protections.

B. Use School Enrollment Data When Possible and Accompany the Collection of Any Individual Data with Proactive Communications with Families, Parental Consent, and Additional Safeguards

To address the risks of unavailable or poor quality data and to protect student privacy, CDT proposes that broadband providers rely on school enrollment data as much as possible. Enrollment data are less sensitive than NSLP or SBP eligibility data and face fewer legal restrictions. Consequently, the Commission should require broadband providers to presume that a child is participating in the NSLP if their school has adopted the CEP. A school's adoption of the CEP excuses it from collecting NSLP applications from families and automatically approves all students at the school for free meals.[20] Thus, all households with students attending CEP schools meet the Act's requirements that at least one member of a household has (1) "applied for" and (2) "been approved" for "benefits under the free and reduced price lunch program."[21] Accordingly, those households should be deemed eligible for the Program.

Although this method of verification might identify more families as eligible for the Program than would occur if they were only permitted to establish individual NSLP eligibility, we believe that risk is outweighed by two other considerations. First, it avoids raising barriers to eligible households' participation in the Program; given the pronounced need for broadband access in the current crisis, providing that access is of paramount importance. Second, this method of verification limits disclosure where possible to less sensitive information, furthering the objectives of connecting students for remote learning and avoiding possible privacy harms that could chill participation in the Program.

[19] 42 U.S.C. § 1758(b)(6); 7 C.F.R. § 245.6(i).
[20] 42 U.S.C. § 1759a(a)(1)(F)(ii), (iv); 7 C.F.R. § 245.9(f)(4)(iii), (iv).
[21] Consolidated Appropriations Act, sec. 904(a)(6)(B).

For students who attend schools that do not participate in the CEP, schools could obtain parental consent to permit the school to disclose the child's individual participation in the NSLP or SBP to broadband providers. Without that consent, disclosure of the child's NSLP or SBP eligibility status by a school may not be permissible under either FERPA[22] or the National School Lunch Act.[23] Further, because schools may not have collected eligibility applications from families for the current school year, individual verification (where necessary) should alternatively include NSLP or SBP eligibility data for the 2019-2020 school year—an approach that has been endorsed by the U.S. Department of Education for programs under the Elementary and Secondary Education Act.[24] Those data should, of course, be considered highly sensitive and treated with safeguards.

For both CEP and non-CEP schools, broadband providers will need to identify the schools where eligible households have children enrolled.[25] This could be accomplished through one of two methods. First, schools may lead the enrollment process. As part of its outreach and publicity program, the Commission could engage schools to promote the Program and ask families to respond if interested in the Program. If the school participates in CEP, it would provide local broadband providers with a list of interested families. If the school does not participate in CEP, it would provide broadband providers with a list of families that have both signaled interest in the Program and consented to disclosure of their NSLP or SBP eligibility.

Alternatively, broadband providers could lead the enrollment process, collecting information, such as the child's or parent's name and the school name, from households applying to the Program to confirm a child's enrollment at a particular institution. That information is not particularly sensitive and its confirmation by schools likely would not implicate student privacy

[22] 20 U.S.C. § 1232g; 34 C.F.R. § 99.30.
[23] 42 U.S.C. § 1758(b)(6); 7 C.F.R. § 245.6(i).
[24] *See* USED, Fact Sheet: State-Administered Programs under the ESEA and the Nationwide Waiver from the U.S. Department of Agriculture to Allow Meal Pattern Flexibility in the Summer Food Service Program and the National School Lunch Program Seamless Summer Option through June 2021 at 4-6 (Jan. 4, 2021), *available at* https://oese.ed.gov/files/2021/01/Fact-sheet-on-USDA-meals-waivers-Jan-2021.pdf (permitting use of the "best available NSLP data, which may be from SY 2019-2020" for programs under Title I).
[25] *See* Public Notice at 7 ("[W]e propose that a provider identify the school it relied on when enrolling a household in the National Lifeline Accountability Database.").

laws, with some exceptions.[26] If the household's school does not participate in CEP,[27] the broadband provider should collect written consent from parents to obtain their children's NSLP or SBP eligibility status from their schools.[28] We suggest that the Commission permit households to initiate the enrollment process through either method, by approaching either a broadband provider or their school.

Regardless of the method of verification, parental consent and compliance with legal requirements must be accompanied by additional safeguards to protect student privacy. Schools should proactively communicate with families about the scope of the Program, what data will be shared to participate in the Program, who will receive it, and how it will be used. When schools share those data with broadband providers, they should enter into written agreements with those providers, identifying the data to be shared and the purpose of the sharing, limiting the data's use and redisclosure, setting time limits for the retention of the data, and establishing minimum administrative and technical safeguards for the data.[29]

II. Explicitly Limit Broadband Providers' Data Collection and Use Under the Program

The Bureau also seeks public comment on permitting broadband providers access to the National Verifier and National Lifeline Accountability Database to verify household eligibility for the Program and track their participation.[30] Under the Commission's proposal, broadband

---

[26] *See* 34 C.F.R. § 99.3, "Directory Information" (describing "enrollment status" as information "that would not generally be considered harmful or an invasion of privacy if disclosed"); *see also* 34 C.F.R. § 99.37 (describing limitations on the release of directory information). If a school cannot verify a student's enrollment, possibly because parents have opted out of the sharing of directory information under FERPA or because state student privacy laws prohibit it, broadband providers may have to obtain parental consent to obtain enrollment status. As noted above, disclosure of NSLP or SBP eligibility always requires parental consent, with limited exceptions likely not applicable here. *See* 42 U.S.C. § 1758(b)(6); 7 C.F.R. § 245.6(i).

[27] A list of schools eligible for or participating in CEP may be obtained from the U.S Department of Agriculture and the Food Research & Action Center. *See Community Eligibility Provision Status of School Districts and Schools by State*, USDA (Mar. 30, 2019), https://www.fns.usda.gov/cn/community-eligibility-provision-status-school-districts-and-schools-state; *Community Eligibility (CEP) Database*, Food Research & Action Center (June 21, 2020), https://frac.org/research/resource-library/community-eligibility-cep-database.

[28] For the requirements for written consent, see 7 CFR 245.6(i); USDA, Limited Disclosure of Children's Free and Reduced Price Meal or Free Milk Eligibility Information (Dec. 7, 1998), *available at* https://www.fns.usda.gov/limited-disclosure-children%E2%80%99s-free-and-reduced-price-meal-or-free-milk-eligibility-information.

[29] See USED, Guidance for Reasonable Methods and Written Agreements (2015), *available at* https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements; USED, Written Agreement Checklist (2015), *available at* https://studentprivacy.ed.gov/resources/written-agreement-checklist.

[30] Public Notice at 4.

providers' tracking of participation through the NLAD would include households that qualify for the Program through the National School Lunch or School Breakfast Programs.[31] The NLAD would consequently include information on students, their families, and their use of government benefits. CDT urges the Commission to limit broadband providers' collection and use of those data.

The National Verifier and NLAD are existing, interconnected services that incorporate data provided by households, broadband providers, and state and federal agencies to determine if a household is eligible for the Lifeline program. Those data include names, the last four digits of consumers' social security numbers, addresses, income, and participation in certain state, tribal, and federal programs.[32] Under Lifeline, consumers may provide information through the National Verifier to verify their eligibility directly, but broadband providers are encouraged to assist them.[33] Broadband providers also separately provide information on potential subscribers to NLAD to ensure that they are eligible for Lifeline.[34] As the Public Notice notes, "such systems must comply with applicable federal requirements on information privacy and information security" such as the Privacy Act of 1974,[35] which limits use of NLAD to specific purposes such as verifying eligibility or engaging in enforcement actions.[36]

CDT encourages the Commission to explicitly limit private entities' collection and use of personally identifiable information under the Program to only that which is necessary to verify eligibility and provide service. These privacy protections will help ensure that consumers are not forced into a false choice between protecting their privacy and using essential connectivity. Data collected by the National Verifier and NLAD such as income or participation in government programs are highly sensitive. Although those data are necessary to operate the Program, their

---

[31] Public Notice at 7 ("[W]e propose that a provider identify the school it relied on when enrolling a household in the National Lifeline Accountability Database.").
[32] *See* 47 C.F.R. § 54.410; *Acceptable Documentation for the National Verifier*, USAC, https://www.usac.org/lifeline/eligibility/national-verifier/acceptable-documentation-for-the-national-verifier/ (listing documentation requirements); *Eligibility Decision Process*, USAC, https://www.usac.org/lifeline/eligibility/national-verifier/eligibility-decision-process/ (listing agencies with automatic and manual data sharing).
[33] USAC, Lifeline National Verifier Plan at 35 (July 2020), *available at* https://www.usac.org/wp-content/uploads/lifeline/documents/nv/plans/National-Verifier-Plan-July-2020.pdf.
[34] *Id.*
[35] Public Notice at 4; *see* 5 U.S.C. § 552a.
[36] FCC Notice of a Modified System of Records, 82 Fed. Reg. 38686, 38689 (Aug. 15, 2017), *available at* https://www.usac.org/wp-content/uploads/about/documents/PrivacyPolicies/fcc-wcb-1.pdf.

misuse or disclosure could invade users' privacy; as such, they deserve protection, just as the FCC requires telecommunications carriers to protect customer information under Title II.[37] Limiting broadband providers' collection and use of data balances the need to provide essential services with the need to protect users' privacy.

Those use and collection limitations are necessary because existing law may not adequately protect users. The Privacy Act, for example, limits governmental data collection and use to specified purposes, but its protections may not extend to private parties such as broadband providers. Similarly, the Commission's existing privacy rules for the Lifeline program only limit providers' queries of the NLAD or the National Verifier[38] and do not limit their collection or use of personal information outside those databases. The Commission's broadband transparency rule likewise only requires that broadband providers disclose their data collection practices but does not actually limit them.[39]

Broadband providers should also be required to delete the personally identifiable information of a user collected under the Program if they choose to terminate participation at the end of the Program. Deletion may be subject to exceptions for data needed to prevent fraud, to engage in reasonable network management practices, or to respond to legal process. Alternatively, carriers may be permitted a limited period to retain data.

III. Avoid Inadvertent Disclosures of Personal Information While Meeting Data Reporting and Accountability Requirements

The Consolidated Appropriations Act permits a broadband provider to avoid certain enforcement actions by the Commission if it "demonstrates that it relied in good faith on information provided to such provider" through the verification methods prescribed by the Act,

---

[37] See 47 U.S.C. § 222; *Consumer Privacy*, FCC https://www.fcc.gov/general/customer-privacy (last visited Jan. 13, 2021).

[38] 47 C.F.R. § 54.404(b)(5) ("Eligible telecommunications carriers may query the Database only for the purposes provided in paragraphs (b)(1) through (b)(3) of this section, and to determine whether information with respect to its subscribers already in the Database is correct and complete."); *Lifeline and Link Up Reform and Modernization*, WC Docket No. 11-42, Third Report & Order, Further Report & Order, and Order on Reconsideration, 31 FCC Rcd 3962, 4013, para. 139 n.391 (Apr. 27, 2016), *available at* https://www.fcc.gov/document/fcc-modernizes-lifeline-program-low-income-consumers ("The National Verifier will only permit queries which facilitate the purposes of the Lifeline program.").

[39] 47 C.F.R. § 8.1 ("Any person providing broadband internet access service shall publicly disclose accurate information regarding the . . . commercial terms of its broadband internet access services . . . .").

including through schools.[40] The Act also requires the Commission to publicly report on spending as required by the CARES Act.[41] As part of its accountability requirements, the Commission also asks, "[S]hould the participating provider be required to measure data usage to ensure the benefit is actually being used? Alternatively, what other measures may the participating provider use to ensure the benefit for which they are reimbursed is actually used . . . ?"[42]

Whatever information it chooses to require for demonstrating good faith or accountability reporting, the Commission should ensure that reporting entities do not inadvertently disclose users' personally identifiable information. Inadvertent or accidental disclosure "can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual[s] to be identified."[43] As the U.S. Department of Education has observed, "Any release of demographic or performance information derived from students' education records, even in aggregate form, carries some level of risk of disclosure of PII, and no statistical disclosure limitation methodology can completely eliminate that risk."[44]

The Commission has not identified the information it will require for accountability reporting, but it should ensure those data do not inadvertently disclose sensitive information about students or households, including their socioeconomic status and participation in government benefits. For example, in its telehealth Order, the Commission identified information it might collect from telehealth providers, including some broken out by "particular geographic area," "class of patients," or "patient group."[45] If similar data were collected and reported for the Emergency Broadband Benefit Program, including from schools, it may inadvertently disclose personally identifiable information. CDT urges the Commission to adopt best practices for the

[40] Public Notice at 12; Consolidated Appropriations Act, sec. 904(j).
[41] Public Notice at 13; Consolidated Appropriations Act, div. O, tit. VIII, sec. 801.
[42] Public Notice at 13.
[43] Privacy Technical Assistance Center, Frequently Asked Questions—Disclosure Avoidance at 1 (2012) [hereinafter FAQ—Disclosure Avoidance], *available at* https://studentprivacy.ed.gov/resources/frequently-asked-questions-disclosure-avoidance.
[44] Letter from Kathleen M. Styles, Chief Privacy Officer, U.S. Department of Education, to John C. White, State Superintendent of Education, Louisiana Department of Education (Apr. 21, 2016) [hereinafter Styles Letter], *available at* https://studentprivacy.ed.gov/resources/sppo-response-louisiana-enrollment-data-and-disclosure-avoidance.
[45] *Promoting Telehealth for Low-Income Consumers*, WC Docket No. 18-213, Report & Order, 35 FCC Rcd 3366, 3414, para. 80 (Mar. 31, 2020), *available at* https://www.fcc.gov/document/fcc-fights-covid-19-200m-adopts-long-term-connected-care-study.

public reporting of data, such as the practices promoted by the U.S. Department of Education and the National Institute of Standards and Technology, including cell suppression, minimum cell sizes, data blurring, rounding, and additional aggregation.[46]

The Commission should also ensure that the proposed Internet usage measurement does not, under any circumstances, involve deep-packet inspection[47] or other means of deriving data about the specific sites, content, or other information that a household accesses through its broadband connection. The Commission should clearly define the scope of the Internet usage measurement, including that a household may be disconnected only if there is no data transmission within a defined period, such as one month. The Commission should also permit households disconnected due to inactivity to challenge the conclusion that they were not using their connections and to reapply for the Program.

IV. Prioritize Marginalized Communities and Students Under the Program Through the Review of Applications, Outreach, and Technical Support

In the Public Notice, the Wireline Competition Bureau seeks comment on important considerations of equity. The Notice asks, "Should the Commission pay special attention to established programs that target groups vulnerable during the pandemic, such as low-income households, Americans living in rural or Tribal areas, communities of color, students, veterans, or the newly unemployed?"[48]

CDT supports the Commission's efforts to focus the Program on vulnerable groups, including low-income and minority communities, especially low-income and minority students.

---

[46] E.g., Styles Letter, *supra* note 44; PTAC, Data De-identification: An Overview of Basic Terms (May 2013), *available at* https://studentprivacy.ed.gov/resources/data-de-identification-overview-basic-terms; FAQ—Disclosure Avoidance, *supra* note 43; Marilyn Seastrom, National Center for Education Statistics, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (Dec. 2010), *available at* https://eric.ed.gov/?id=ED514095; Marilyn Seastrom, NCES, Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records (Nov. 23, 2010), *available at* https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601; Erika McCallister et al., NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Apr. 2010), *available at* https://csrc.nist.gov/publications/detail/sp/800-122/final.

[47] "Deep-packet inspection" occurs when broadband providers look beyond the bare minimum of data they need to direct internet traffic to its destination and begin to look at the content of that traffic. *See Applying Communications Act Consumer Privacy Protections to Broadband Providers*, CDT (Jan. 20, 2016), https://cdt.org/insights/applying-communications-act-consumer-privacy-protections-to-broadband-providers/

[48] Public Notice at 5.

This focus can be accomplished by prioritizing review (and funding) for applications for participation in the Program by broadband providers in areas where they serve communities that are low-income, minority, or with large concentrations of school-aged children. That focus may also be accomplished by targeting publicity efforts and technical support at those broadband providers and communities.

V. Fully Enable Students' Participation in the Program by Providing Cybersecurity and Digital Literacy Training and Clarifying Disparate Applications of the Monitoring Requirement of the Children's Internet Protection Act

CDT also urges the Commission to take this opportunity to address two other issues to ensure that students and families may fully connect with educational opportunities online. First, increased connectivity requires training on basic cybersecurity and digital literacy issues. Research from Michigan State University demonstrates that "students who do not have Internet access at home have significantly lower digital skills" in using the Internet, social media, and telecommunications than their peers.[49] Yet, less than half of parents say their schools have discussed how to protect student privacy with them.[50] Consequently, the Commission should provide schools and households with resources on cybersecurity and digital literacy to navigate the online world. Some resources already exist and have been provided by governmental and nonprofit entities as well as public-private partnerships.[51]

Second, we believe that the Commission should clarify the "monitoring" requirement of the Children's Internet Protection Act (CIPA). That requirement has been construed broadly by institutions to require scanning of student messages, tracking student browsing history, or maintaining access to the microphones and cameras on school-issued devices.[52] This over-broad

[49] Keith N. Hampton et al., Michigan State University, Broadband Gap and Student Performance Gaps at 8, 30-32 (2020), *available at* https://quello.msu.edu/broadbandgap/.
[50] CDT, Research Slides: Teacher, Parent, and Student Views on Education Data, Technology, and Student Privacy at 29 (2020), *available at* https://cdt.org/press/research-shows-teachers-parents-students-need-more-support-to-protect-privacy-and-advance-digital-equity/.
[51] *E.g.*, *OnGuard Online*, Federal Trade Commission, https://www.consumer.ftc.gov/features/feature-0038-onguardonline (last visited Jan. 11, 2021); *Digital Citizenship Curriculum*, Common Sense, https://www.commonsense.org/education/digital-citizenship/curriculum (last visited Jan. 11, 2021); *STOP. THINK. CONNECT.*, stopthinkconnect.org (last visited Jan. 11, 2021).
[52] E.g., Mark Keierleber, *Minneapolis School District Addresses Parent Outrage Over New Digital Surveillance Tool as Students Learn Remotely*, The 74 (Oct. 28, 2020), https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely/; Nader Issa, *CPS*

surveillance is harmful and not required by the plain text of CIPA, which mandates only that schools "enforc[e] a policy of Internet safety for minors that includes monitoring the online activities of minors."[53] That language does not reasonably extend to the drastic measures that some institutions have implemented, as CIPA expressly disclaims that it requires the "tracking" of any user.[54]

This rulemaking is an appropriate time to clarify the scope of CIPA's monitoring requirement. Although the proposed Emergency Broadband Benefit Program does not include any monitoring requirement, many students are now using school-issued devices equipped with varying monitoring tools to connect from home. This creates an unreasonable disparity, premising students' and families' privacy on which state or federal program they use to connect to their education. The Commission should clarify that CIPA's monitoring requirement is narrow and may be achieved without unduly treading on student privacy.

Conclusion

CDT applauds the Commission's proposed Emergency Broadband Benefit Program, a major step forward to close the homework gap and bridge the digital divide. That work can be accomplished while protecting students' and families' privacy. Privacy protective measures include verifying participation in the NSLP or SBP through enrollment data, addressing cybersecurity, digital literacy, and monitoring, limiting broadband providers' collection and use of data, avoiding inadvertent disclosures in reporting accountability data, and promoting equity through the Program.

Teachers Could Look Inside Students' Homes—Without Their Knowledge—Before Fix, Chicago Sun-Times (Oct 5, 2020), https://chicago.suntimes.com/education/2020/10/5/21497946/cps-public-schools-go-guardian-technology-privacy-remote-learning;

[53] 47 U.S.C. § 254(h)(5)(B)(i).

[54] Children's Internet Protection Act, Pub. L. No. 106-554, sec. 1702, 114 Stat. 2763, 2763A–336 (2000), *available at* https://www.govinfo.gov/content/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf ("Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user."); see also Dian Schaffhauser, *K–12 Data Privacy During a Pandemic*, T.H.E. Journal (Sept. 10, 2020), https://thejournal.com/articles/2020/09/10/k12-data-privacy-during-a-pandemic.aspx.